CMS

Illinois Department of

Central Management Services

State of Illinois

Public Key Infrastructure

Certification Practice Statement

Version 1.4

May 11, 2004

Public Version

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
1.4	June-24-2004	Staff	Sanitized for web	Sections removed

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

This Certification Practice Statement (CPS) describes the practices of the Certificate Authority (CA) operated by the State of Illinois Central Management Services ("State"). This CPS is applicable to all entities with relationships with the State CA, including end users, Registration Authorities (RAs) and Local Registration Authorities (LRAs). This CPS provides those entities with a clear statement of the practices and responsibilities of the State CA, as well as the responsibilities of each entity in dealing with the State CA.

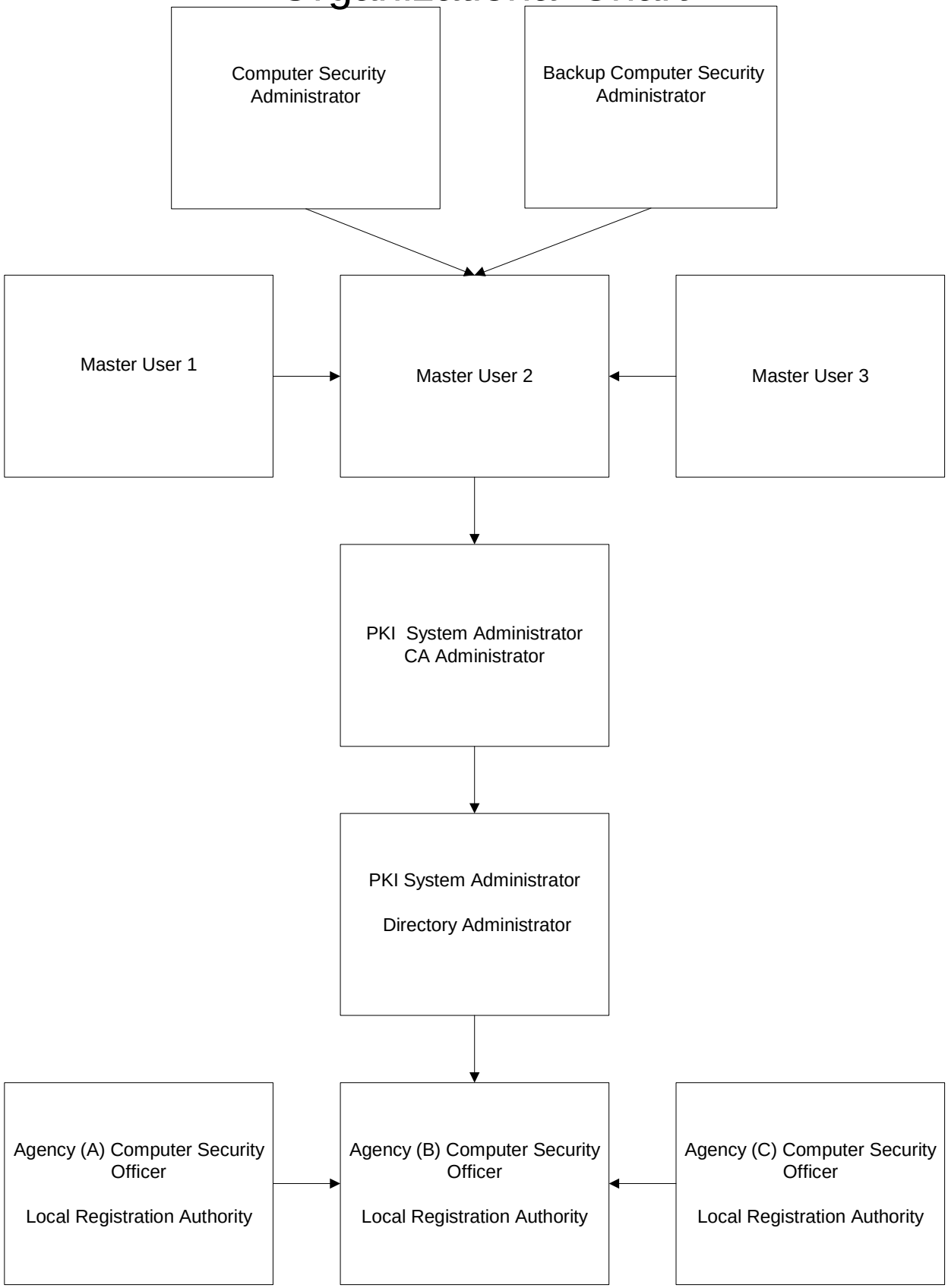
1.1.1 Roles and Responsibilities

Section 25-105 of the Illinois Electronic Commerce Security Act (5 ILCS 175/25-105provides that the Illinois Department of Central Management Services (CMS) shall have the exclusive authority to specify the policies and procedures for the issuance and use of digital signatures by State Agencies. The Certificate Policy (CP) and the Certification Practices Statement (CPS) are CMS's written description of the policies and procedures for the issuance and use of digital signatures. The Director of CMS has delegated responsibility for implementation and maintenance of the CP and the CPS to the State of Illinois Certificate Policy Authority (PA).

The PA shall be comprised of representatives of participating units of Illinois State government. The Director of CMS shall have the exclusive authority to appoint and remove members of the PA. Members of the PA (or their designees) shall have the authority to implement, maintain, and modify the CP and the CPS, and shall perform all other duties required of them by the terms of the CP and the CPS.

There is created by the CP and this CPS a State of Illinois Operational Authority (OA.) The Director of CMS shall have supervisory responsibility for the OA. The OA shall be responsible for interpretation of the certificate policies as stated by the PA, the creation and management of the CPS, and the correct operation of the State PKI, in accordance with the provisions of the CP and the CPS. The CMS Security Administrator shall oversee the operations of the State PKI. The CMS PKI registration authority (RA) shall manage the operations of the State PKI. CA functions described in the CP and the CPS shall be performed by PKI Administrators. RA functions described in the CP and CPS may be delegated to Local Registration Authorities (LRAs.) Figure 1 illustrates the CMS organizational structure relating to the operation and management of the State CA.

State Of Illinois CMS PKI Organizational Chart



This CPS is managed by the State of Illinois Operational Authority (OA) and adheres to the policies established by the State of Illinois Policy Authority (PA). Contact information for these authorities is provided in section 1.4 below.

1.2 IDENTIFICATION

This CPS is called the State of Illinois Certificate Authority Certification Practice Statement.

The State CA issues Certificates for use in verification of digital signatures and Certificates for use in encryption. The State CA supports several Certificate Policies that cover both of these applications. Practices that differ from this policy are clearly indicated in this CPS.

1.3 COMMUNITY AND APPLICABILITY

The sub-sections that follow describe in general terms, the functions of the major components of the PKI.

1.3.1 Certificate Authorities

The State operates a single CA, which issues user Certificates to State Employees and other entities that conduct business with the State.

The State CA is operated using Entrust release 5.0 software and the CA is represented in the architecture by Entrust/Authority™. The authorized State personnel access Entrust/Manager via the Entrust/RA interface to initiate and perform CA functions.

1.3.1.1 Figure 2 illustrates the relationships of CMS individuals to PKI roles and Entrust user privileges.

State Individual	PKI Entity/Role	Entrust Role/Privilege
	PA Chair & OA Head	N/A
	CA operator	Security Officer
	CA operator	Security Officer
	Contact Point	Master User 1
	Contact Point	Master User 2
	Contact Point	Master User 3
PKI System Administrator Registration Authority	CA operator	Certificate Authority Administrator
PKI System Administrator Directory Administrator	CA operator	Registration Authority Administrator
Agency Assigned Individual	LRA operator	Entrust user

State Employees and Business Partner Users	Subscriber Relying party	Entrust user

Figure 2: Roles and Privileges

Where necessary, this CPS distinguishes the different users and roles accessing Entrust/ Authority™ for CA functions. Where this distinction is not required, the term CA is used to refer to the total CA entity, including the software and its operations.

1.3.2 Registration Authorities

1.3.2.1 Registration Authority

The Registration Authority has privileges that are a proper subset of Security Officer privileges as outlined in section 5.2.1 of this CPS. The State RA makes use of authorized individuals to function as Local Registration Authorities to verify the identity and roles of End Entities throughout the various State agencies and business partners, in accordance with the State of Illinois Certificate Policy.

1.3.2.2 Local Registration Authority

Each Agency will designate one or more individuals to perform the role of the Local Registration Authority within that agency, and has privileges that are a proper subset of Security Officer privileges as outlined in section 5.2.1 of this CPS. In this CPS, the term Local Registration Authority (LRA) is used to refer to an individual performing RA functions, while RA is used to refer to the total RA entity, including the software and its operations.

1.3.3 Applicability

This CPS is applicable to all Certificates issued by the State CA, including those issued under the 'Certificate Policy for Digital Signature and Encryption Applications' policy.

The practices described in the CPS apply to the issuance and use of Certificates and Certificate Revocation Lists (CRLs) for users within the State CA domain.

1.3.3.1 Suitable Applications

Each of the Certificate Policies supported by the State CA, and covered by this CPS, identifies the suitable applications for that Certificate Policy.

1.4 CONTACT DETAILS

This CPS is administered by the State PKI Operational Authority (OA) and is based on the policies agreed to by the State PKI Policy Authority (PA).

2. GENERAL PROVISIONS

2.1 PUBLICATION AND REPOSITORIES

CMS shall maintain a Certificate Repository containing information pertaining to State Certificates.

2.1.1 Publication of CA Information

This detailed CPS is not published publicly. The edited version is available publicly.

The following PKI information is published in the State Directory:

- all encryption public key Certificates issued by the State CA to PKI users;
- all revocations of PKI user public key Certificates performed by the State CA;

2.1.2 Frequency of Publication

This CPS is re-issued and published as necessary.

Certificates are published in the Directory as they are issued.

CRLs are published in the Directory as they are issued.

2.1.3 Repositories

The repository for this CA is provided by an X.500 directory system. The protocol used to access the Directory is the Lightweight Directory Access Protocol (LDAP) version 2 or higher.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

Subject to the requirements noted below, applications for State Certificates may be communicated from the applicant to the State RA or a State LRA and authorizations to issue State Certificates may be communicated from an authorized State LRA to the State CA, (1) electronically, provided that all communication is secure, or (2) in person.

The State CA expects to process three types of registrations:

- Web registration (both in-state and out-of-state recipients).
- Face-to-face registration authorized by the State RA or a State LRA.
- Bulk registration. Using a secure means determined on a case by case basis, authorized LRAs will authorize the issuance of Certificates to large groups of Subscribers that they have registered and communicate these to the State RA.

3.1.1 Types of Names

Names for Certificate issuers and Certificate subjects are of the X.500 Distinguished Name (DN) form.

All attributes are as defined in ITU-T Recommendation X.521.

3.1.2 Need for Names to be Meaningful

The value of the commonName attribute used is the name by which the Certificate subject is commonly known within the client organization.

3.1.3 Uniqueness of Names

Names are unambiguously defined for each object in the naming hierarchy. The serialNumber attribute within the DN is used to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity.

3.1.4 Name Claim Dispute Resolution Procedures

By incorporating Subject names into State Certificates, the State does not determine whether the use of the Subject name infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property or other rights of any person, entity or organization. the State neither acts as an arbitrator nor provides dispute resolution between Subscribers and third party complainants in respect to disputes in relation to the registration or use of a Subject name in a State Certificate. This CPS does not bestow any procedural or substantive rights on any third party complainant in respect to the Subject name in a Certificate. The State shall in no way be precluded from seeking legal or equitable relief (including

injunctive relief) in respect to any dispute between a Subscriber and third party complainant or in respect to any dispute between a Subscriber and the State arising out of the Subject name in a State Certificate. The State shall have the right to revoke a State Certificate upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of the State Certificate or State Certificates containing a Subject name in dispute. Since both the commonName and serialNumber attributes are used to create the RDNs for Certificate subjects, such disputes are expected to be rare.

3.1.5 Method to Prove Possession of Private Key

Digital Certificates bind a public key to the identity of the individual to assure Relying Parties that encryption or signing performed by the private key was done by the individual whose public key appears on the Certificate. This requires that an individual safeguard their .epf file and Entrust password and that the CA require proof of possession of the private key before creating and signing a Certificate containing the associated public key. Proof of possession of private key is handled automatically by the operations of the PKIX.

For the signature private key, a PKIX operation initiated by the Subscriber is digitally signed using the signature private key itself.

For the decryption private key, this key is transferred to the Subscriber, together with the corresponding Certificate, in a PKIX operation which is digitally signed by the State CA.

3.1.6 Authentication of Individual Identity

The following sections detail the registration process to be used for issuance of State Certificates:

- Face to Face Registration

  The Subscriber will present themselves in person along with a valid form of photo identification (either a State of Illinois Driver's License or a Secretary of State Identification Card) and one other form of Id to either the RA or an LRA. The RA or LRA will validate the information and sign and date the form, which at a minimum will include:

  - full name.
  - Driver's license number or Secretary of State Identification Number.
  - Shared secret information for key recovery.

  If an LRA conducts the registration, they will then securely forward the information on to the RA, who will then generate the certificates.

  If an LRA exists for the subscriber, the reference number and authorization code are encrypted, signed and emailed to the LRA. If no LRA exists, then one part of the necessary authorization credentials is emailed and another will be provided via some "out of band" method. The RA or LRA is responsible to provide the necessary credentials to subscribers who will be "desktop users". These two pieces of information are required for the Subscriber to authenticate and initialize themselves with the CA at their initial login.

If a subscriber is to be a "roaming user", then the digital certificate and the profile are both created under the user's control by the CA and the profile name and password are securely transmitted to the LRA or the subscriber as described above.

A face-to-face registration results in a level 2 authorization level unless a background check is also performed. In this case, a level 3 assurance level is assigned.

All registration forms will be securely retained indefinitely.

All trusted roles must have at least a level 3 assurance level.

- Web registration

  Agencies can choose to include a link in their developed web applications that will route the subscriber to a State web page. This web page would allow the subscriber to fill out an on-line form and obtain a digital certificate. The subscriber will provide information that the Agency's application deems necessary as well as information found on the subscriber's drivers license and shared secret information. This driver's license information is then verified against the driver's license database housed at the Secretary of State. Currently, the information verified is the driver's license number and the weight as shown on the driver's license. If this information matches, then a digital certificate will be issued to the subscriber and they will be returned to the Agency's application that they started with. The shared secret information will be stored in a secure DB2 database housed at CMS for use in later key recovery operations.

  An out-of-state registration process has been added to the web registration model. Under this process, non-Illinois residents can request a State of Illinois digital certificate by going to the normal registration web site and choosing the "out-of-state" option. This option directs them to download and print an application form, and to take it to a notary public where their identification credentials are inspected. Once the form is notarized, it is mailed to the Operational Authority for processing. Once the activation codes are created by the Operational Authority, the activation codes are returned to the requestor via email and one "out-of-band" method. They are then directed to go to another web site and enter the activation codes, thus creating the certificate.

  The web registration model will only result in a level 1 assurance level.

- Other registration methods may be used that are consistent with the requirements of the CP and created with the approval of the Policy Authority.

3.1.7 Authentication of Devices or Applications

Application for a device or an application to be an End-Entity must be made by an individual to whom the device or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant follows 5.2.4 of the CP as if the organization or individual were applying for a Certificate on their own behalf. In addition, the RA or PA must verify the authority of the individual to receive Certificates for that device or application.

3.2 ROUTINE REKEY

Certificates issued by the State CA (both device certificates and certificates for individuals) will be setup to automatically renew. All encryption and digital signature key pairs will expire at the end of the Certificate validity period. Keys enter what is referred to as a transition period when they approach their lifetime end.

Once a subscribers keys enter the transition period, the CA will automatically attempt to perform a key update. This is a transparent operation that should cause no interruption of operation. Failure of the Subscriber to successfully connect to the CA to complete this key update during the transition period will result in their Certificate expiring and the Subscriber having to repeat the authentication process defined in section 3.1.6 of this CPS.

For all Certificate renewal requests, the Certificates are renewed using PKIX operations invoked by Entrust/Authority™. Authentication of the individual's identity as defined in section 3.1.6 of this CPS need not be repeated. However, reauthentication of an individual's identity shall occur as described in section 5.6.2 of the CP.

For cross-certification relationships, no automatic key update process is applied. If the State PA determines that a cross-certification agreement is to extend beyond the original period, a new cross-certificate is issued, prior to expiration of the current one. The same identification and authentication process used for initial cross-certification agreements applies to the issuance of new keys.

3.3 RECOVERY AFTER REVOCATION

For users whose Certificates have been revoked, recovery after revocation will generally not be permitted until the identification and authentication requirements for initial registration described in section 3.1.6of this CPS are repeated. Local Registration Authorities may allow exceptions in the following situations:

- A user is temporarily unable to present themselves in person (e.g. on extended travel) and the revocation was not due to a key compromise.

3.4 AUTHENTICATION OF REVOCATION REQUEST

Requests by a Trusted Role to revoke a Certificate require Administrator privilege credentials to be supplied at login to Entrust/Authority™ before revocation requests can be serviced. Requests by the Subscriber to revoke their own Certificate require one of the following identification and authentication mechanisms prior to a Trusted Role initiating an online request:

- Subscriber presents themselves in person along with their photo id card;
- digitally signed email sent from the Subscriber to a Trusted Role.

Requests to revoke device and application certificates must be provided (via signed email or in person) by the LRA or Security Officer of the responsible agency.

A trustworthy, automated revocation process may replace or supplement the above-described manual process.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Both the Reference Number and Authorization Code are required for the individual to initially login to the PKI system as a new user unless the user is created as a roaming user. A digital signature key pair is generated by the software on the client desktop and a Certificate request is sent to Entrust/Authority™ using the PKIX protocol.

4.2 CERTIFICATE ISSUANCE

The PKIX Certificate request is digitally signed by the Subscriber using the newly generated signing key. Upon receipt of a valid request, the State CA automatically generates an encryption key pair and issues both a signature verification public key Certificate and an encryption public key Certificate for that Subscriber. Both Certificates and the decryption private key are returned to the Subscriber using the PKIX-CMP protocol. A self-signed root CA certificate is securely delivered to subscribers using PKIX-CMP during the certificate issuance process.

4.3 CERTIFICATE ACCEPTANCE

As the PKIX operations are themselves secured and the two entities (Subscriber and CA) authenticated, successful completion of the PKIX request and response operations constitutes acceptance by the user of the resulting public key Certificates. By accepting the State Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the State Certificate are true.

4.4 CERTIFICATE UPGRADE

Digital certificates can be obtained through an Internet registration process that results in a low level (level 1) assurance level. A certificate can be upgraded if necessary.

4.5 CERTIFICATE REVOCATION AND SUSPENSION

4.5.1 Procedure for Revocation Request

If a PKI Administrator is initiating a revocation request, they login by providing the appropriate credentials to Entrust/RA and initiate a revocation request to Entrust/ Authority™ for execution.

If an End Entity, who is the subject of the Certificate to be revoked, or one of the other individuals identified in section 5.2.1 of this CPS, is initiating the revocation request, the initial request is made off-line. If possible, the individual presents himself or herself in person along with a photo id card. If that is not possible (e.g. the Subscriber is on extended travel), a digitally signed email request can be sent to the RA. Upon receipt of a valid request, a PKI Administrator will login by providing the appropriate

credentials to the Entrust/RA system and initiate a revocation request to Entrust/Authority™ for execution.

In all cases, a record is retained in the software audit trail of the online request and a paper record of any offline request is retained by the OA.

4.5.2 Revocation Request Grace Period

In the case of key compromise, suspected key compromise, or dismissal for cause, the revocation request must be placed within no more than 8 hours of the detection of the compromise or suspected compromise.

Revocation requests for other revocation reasons must be placed within 48 hours of the change.

The State CA is not liable for any damages due to the failure of a Subscriber to meet these requirements for requesting revocation.

4.5.3 Circumstances for Suspension

The State CA does not suspend Certificates.

4.5.4 Who Can Request Suspension

No stipulation - this section intentionally left blank.

4.5.5 Procedure for Suspension Request

No stipulation - this section intentionally left blank.

4.5.6 Limits on Suspension Period

No stipulation - this section intentionally left blank.

4.5.7 CRL Issuance Frequency

As a minimum, the State CA issues CRLs and ARLs on a 24-hour interval. The CRLs and ARLs are issued 7 days per week. On an exception basis, CRLs and ARLs may also be issued between these intervals (e.g.: upon detection of a serious compromise situation or a certificate revocation).

4.5.8 CRL Checking Requirements

Section removed for security purposes

4.5.9 On-line Revocation/Status Checking Availability

The State CA does not support on-line revocation/status checking other than via CRLs as described in section 4..5.8 of this CPS.

4.5.10 Special Requirements Key Compromise

In any key compromise situation, a report must be filed with the State PKI RA, or equivalent, indicating the circumstances under which the compromise occurred. If accidental, on the part of the Subscriber, no further action is required. Otherwise the State PKI Administrator, or equivalent, will determine if a possible follow up investigation, potential action, or reauthentication is required in accordance with the existing IT Security Policy.

After revocation, the Subscriber cannot log onto the system and must be set up by a RA for key recovery.

4.6 SECURITY AUDIT PROCEDURES

4.6.1 Types of Event Recorded

Section removed for security purposes.

4.6.2 Frequency of Reviewing Audit Log

The audit trail is reviewed for policy violations or other significant events at least once per week.

4.6.3 Retention Period for Audit Log

The audit trails are retained for a minimum of five years under normal operation.

4.6.4 Protection of Audit Log

Security Administrators, Certificate Authority Administrators and Directory Registration Authorities are capable of viewing and processing audit trail files.

4.6.5 Audit Log Backup Procedures

Section removed for security purposes.

4.6.6 Audit Collection System

The audit trail accumulation system is internal to Entrust/Authority™ software system.

4.6.7 Notification to Event-causing Subject

State CA personnel causing audit events should receive notification, as appropriate, via the Entrust/RA interface.

Users causing audit events receive notification, as appropriate, via the Entrust/Entelligence ™ software interface. Such notifications are conveyed from Entrust/Authority™ to Entrust/Entelligence ™ using the PKIX protocol.

4.7 RECORDS ARCHIVAL

Section removed for security purposes.

4.7.1 Types of Event Recorded

Section removed for security purposes.

4.7.2 Retention Period for Archive

Section removed for security purposes.

4.7.3 Protection of Archive

The Entrust/Authority™ database is encrypted and protected by master keys. Integrity of the audit trail is as described in this CPS.

The archive data will be digitally signed by the State's CA. This will provide an integrity check that can be used to verify that the data has not been modified.

4.7.4 Archive Backup Procedures

Section removed for security purposes.

4.7.5 Archive Collection System

The archive collection system (backup facility) for the Entrust/Authority™ database is internal to the Entrust/Authority™ system.

The archive collection system (backup facility) for the audit trail files is described in section 5.9.5 of the CP.

The archiving of both data stores onto separate media and secure storage of that media is external from the Entrust/Authority™ system.

4.7.6 Procedures to Obtain and Verify Archive Information

Refer to CMS Security Policy.

4.8 KEY CHANGEOVER

Section removed for security purposes.

4.9 COMPROMISE AND DISASTER RECOVERY

In the event of a disaster or serious compromise, the following steps, as a minimum, are taken to recover a secure environment:

4.9.1 Computing Resources, Software, and/or Data are Corrupted

All operations will be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage.

4.9.2 CA Public Key Is Revoked

Section removed for security purposes.

4.9.3 CA Private Key Is Compromised

Section removed for security purposes.

4.9.4 Secure Facility after a Natural or Other Disaster

All operations will be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage.

4.9.5 System Backup Procedures

Section removed for security purposes.

4.10 CA CESSATION OF SERVICES

In the event that the State CA ceases operation or is otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation;
- All CAs with which cross-certification agreements are current at the time of cessation will be informed so that cross-Certificates to the State CA may be revoked;
- All State Certificates issued by the State CA shall be revoked no later than the time of cessation; and
- All current and archived State identity proofing, Certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be archived according to the State data archive policy.

4.11 MULTIPLE CERTIFICATES CAUSED BY DIFFERENT REGISTRATION METHODS

Section removed for security purposes.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

The focus of physical security controls is to minimize exposure from environmental hazards and malicious actions that could harm data or information, severely delay the timeliness of processing or threaten the safety of personnel.

5.1 CA PHYSICAL SECURITY CONTROLS

Section removed for security purposes.

5.1.1 Hardware and Software Security Controls

All hardware and software updates or installations shall be purchased or developed in the same manner as the original equipment, and will be installed by trusted and trained personnel. In doing so, a formal configuration management methodology shall be followed for such installs or ongoing maintenance of the CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The State CA is represented by the Entrust/Authority software. The main administrative interfaces to Entrust/Authority are the Entrust/Registration Authority and Master Control. These interfaces are used by PKI entities with special privileges, to perform the CA and RA functions in the State PKI. These roles and associated privileges are described below:

At the State, there are three Master Users. Their PKI Master User passwords are documented and stored in a safe approved by the State OA. The Master Users have authority to:

- Maintain Entrust/Authority services (consisting of Administration Services, Key Management Services, and Directory Services) plus the Entrust/Authority database.
- Recover Security Administrator and Security Administrator Backup in the event they have forgotten their passwords.
- Recover the Entrust Administration services, in the event its profile becomes damaged.
- Backup, re-encrypt and restore from backup as necessary, the Entrust Manager database.

In the Entrust context, the State personnel who specify the State CA's security polices are Entrust Security Administrators. The Entrust Security Administrator created during the installation of the Entrust Authority is the 'First Officer'. The First Officer, drawing from selected State personnel, creates additional Entrust Security Administrators. The main role of the Security Administrators is to set and administer the State's security policy as it applies to all PKI Subscribers. Security Administrators use Entrust/Registration Authority as their interface to Entrust/Authority and have the following privileges:

- Set the security policy for the CA, and alter it.

- Add, delete and deactivate other Security Administrators, Local Registration Authorities, Directory Administrators and Subscribers.
- Authorize sensitive operations, such as adding and deleting Security Administrators and Certificate Authority Administrators.
- Process audit logs.
- All Certificate Authority Administrator privileges.

In the Entrust context, the State personnel and any others who are RA's have Administrator privileges. These are:

- Add, delete and suspend Subscribers.
- Manage key recovery for Subscribers.
- Revoke Subscriber Certificates.
- Change Subscriber DNs.

The State CA staff performs the role of System Administrator and has root access to the CA operating system. The Operation Authority will perform routine self-assessments of security controls.

5.2.2 Number of Persons Required per Task

- All Security Administrators operations need one Security Administrator authorization. Certain functions, such as activation of the CA Private Key, will be protected by multi-person controls (see Section 6.2 of the CP).

5.2.3 Identification and Authentication for Each Role

Refer to section 3.1.6 of this CPS for identification and authentication procedures for individuals filling the Trusted Roles in the State PKI.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Personnel Security Controls for Certification Authority

Section removed for security purposes.

5.3.2 Personnel Security Controls for Registration Authority & LRA's

The RA shall periodically conduct random background checks of LRAs, to assure compliance with the ongoing reporting requirements of this section.

A previously conducted background check will be accepted as long as it is no more than 2 years old at the time of applying to become an LRA.

LRA privileges may be denied, suspended, or revoked at the discretion of the RA. Reasonable notice and opportunity for hearing shall be provided, as warranted by the specific circumstances. Hearings shall be

conducted by the PA, which shall have the authority to uphold or overrule actions by the RA denying, suspending or revoking LRA privileges. The RA may deny, suspend, or revoke LRA privileges for good cause shown, including but not limited to:

- Commission or conviction of a criminal offense involving moral turpitude;
- Failure to cooperate fully in any investigation by the RA or PA;
- Failure to comply with the CP and the CPS;
- Separation from, or reassignment within the sponsoring governmental entity;
- Refusal or inability to diligently complete the obligations of an LRA.

LRAs shall:

- Read and understand the CMS document entitled “Local Registration Authority Administrative Rules”.
- Read and understand the CMS document entitled “Local Registration Authority Guidelines for Registration”.

6. TECHNICAL SECURITY CONTROLS

The State will implement comprehensive technical controls for the State PKI, will ensure that the system is continuously operated within the approved security parameters and that all required technical controls remain in place and properly configured.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The CA signing key pair is created during the initial start up of the Entrust/Master Control application and is protected by the CA master key.

The software key generation process is designed to comply with FIPS 140-1 level 1. With a hardware token the generation process may be compliant with higher levels of FIPS validation.

For all the State PKI key pairs the encryption key pair and the corresponding encryption Certificate are created by Entrust/Authority™. The digital signature key pair is generated by the client software or in some cases by a hardware token. Keys generated by software may be stored in a software file or on a hardware token. These products contain at least a FIPS 140-1 approved cryptographic module.

6.1.2 Private Key Delivery to Entity

The private decryption key is provided securely to the user via PKIX protocol exchange between Entrust/Authority™ and Entrust/Direct™ or Entrust/Entelligence™ or between Entrust/Authority™ and the user's hardware token. The authorization code is used to derive a MAC key which is then used to provide authentication and integrity protection on the session. For the digital signature key pair, as the key pair is generated by the user, no delivery of the private key is required.

6.1.3 Public Key Delivery to Certificate Issuer

The encryption key pair is created by Entrust/Authority™, and a copy of the public encryption key is placed in the Directory and delivery of the encryption public key to the Certificate issuer is required. The signature verification public key is delivered securely to Entrust/Authority™using the PKIX protocol.

6.1.4 CA Public Key Delivery to Users

The CA verification public key is delivered in a CA Certificate to users using the PKIX protocol. Authenticity and integrity protection is based on a MAC key derived from the authorization code.

6.1.6 Key Sizes

Section removed for security purposes.

6.1.7 Public Key Parameters Generation

Section removed for security purposes.

6.1.8 Parameter Quality Checking

Section removed for security purposes.

6.1.9 Hardware/software Key Generation

Most PKI users will have the digital signature key pair generated in software. Some Entrust users may have hardware tokens which generate this key pair. The keys generated by the State CA are generated in software in Entrust/Authority™ with the exception of the CA private signing key which is generated on the Luna CA 3 token.

6.1.10 Key Usage Purposes

Certificates issued by the State CA contain the key Usage Certificate extension restricting the purpose to which the Certificate can be applied.

The digital signature key pair is used to provide authentication, integrity and support for non-repudiation services.

The encryption key pair is used to protect a symmetric key used to encrypt data, and as such provides confidentiality services.

The State CA signing key is used to sign Certificates, CRLs and ARLs issued by that CA.

The PKIX session keys are used to provide secure communications for key management operations.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The cryptographic module used by Entrust software to generate keys is designed to comply with FIPS 140-1 level 3. Some users have hardware tokens which generate keys and these may comply with higher levels of FIPS validation.

6.2.2 Private Key Multi-person Control

Section removed for security purposes.

6.2.3 Private Key Escrow, Backup and Recovery

Escrow of private keys by an external third party is not performed.

6.2.4 Private Key Activation and Entry into Cryptographic Module

Section removed for security purposes.

6.2.5 Method of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the subject logging out from the Entrust application or automatically after a preset period of time configured in Entrust/Authority. The preset timer is controlled from Entrust/Authority by the Security Administrator.

6.2.6 Method of Destroying Private Key

All sensitive keys in memory are overwritten with zeros when no longer used. Permanent destruction of private keys is achieved with secure delete operations.

6.2.7 Cryptographic Module Protection

All hardware cryptographic modules shall be removed and stored in a secure location when not in use.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

Section removed for security purposes.

6.3.2 Usage Periods for the Public and Private Keys

Section removed for security purposes.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

- Passwords are required by all entities logging on to Entrust components. Entrust applies a stringent set of rules to each password to ensure it is secure.

6.4.2 Activation Data Protection

Section removed for security purposes.

6.4.3 Other Aspects of Activation Data

Section removed for security purposes.

6.5 COMPUTER SECURITY CONTROLS

Section removed for security purposes.

6.6 LIFE-CYCLE SECURITY CONTROLS

The effectiveness and appropriateness of the security settings described in this CPS are reviewed as part of the audit procedures specified in the CP.

6.7 NETWORK SECURITY CONTROLS

Section removed for security purposes.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The Entrust software cryptographic module is validated to comply with FIPS 140-1 level 1. The cryptographic module(s) used for CA, RA, and LRA functions may be evaluated at FIPS 140-1 level 3 using optional cryptographic hardware modules.

7. CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

Section removed for security purposes.

7.1.1 Version Number(s)

Certificates issued by this CA are issued with the version number set to v3.

7.1.2 Certificate Extensions

Section removed for security purposes.

7.1.3 Algorithm Object Identifiers

Section removed for security purposes.

7.1.4 Name Forms

Section removed for security purposes.

7.1.5 Name Constraints

Name constraints are not used in this PKI.

7.1.6 Certificate Policy Object Identifier(s)

Section removed for security purposes.

7.1.7 Usage of Policy Constraints Extension

Policy constraints are not used in this PKI.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy qualifiers are not used in this PKI.

7.1.9 Processing Semantics for the Critical Certificate Policy Extensions

Section removed for security purposes.

7.2 CRL PROFILE

Section removed for security purposes.

7.2.1 Version Number(s)

CRLs issued by this CA are X.509 version 2 CRLs.

7.2.2 CRL Extensions

Section removed for security purposes

8. POLICY ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Changes to items within this CPS which, in the judgment of the OA and PA, will have no/minimal impact on the users managed by this CA, may be made with no change to the CPS version number and no notification to the users.

Changes to the Certificate Policies supported by this CPS as well as changes to items within this CPS which, in the judgment the OA and PA may have significant impact on the users managed by this CA, may be made with 30 days notice to the user community and the version number of this CPS must be increased accordingly.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

The State CA shall make available copies of the CP both online and in hard copy form. The dissemination of the CPS will be made at the discretion of the Policy Authority.

8.3 CPS APPROVAL PROCEDURES

The State PA approves this CPS. The State PA must approve any subsequent changes prior to promulgation.

9. ACRONYMS

ARL	Authority Revocation List
CA	Certificate Authority
CAA	Certificate Authority Administrator
CCTV	Closed circuit television
CIT	Corporate Information Technology
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAP	Directory Access Protocol
DES	Data Encryption Standard
DN	Distinguished Name
DNS	Domain Name Server
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
FIPS	Federal Information Processing Standard
HR	Human Resources
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
ISO	Information Security Officer
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
OA	Operational Authority
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509

PMA	Policy Management Authority
PUB	Publication
RA	Registration Authority
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TRA	Threat and Risk Assessment
URI	Uniform Resource Identifier
URL	Uniform Resource Locator